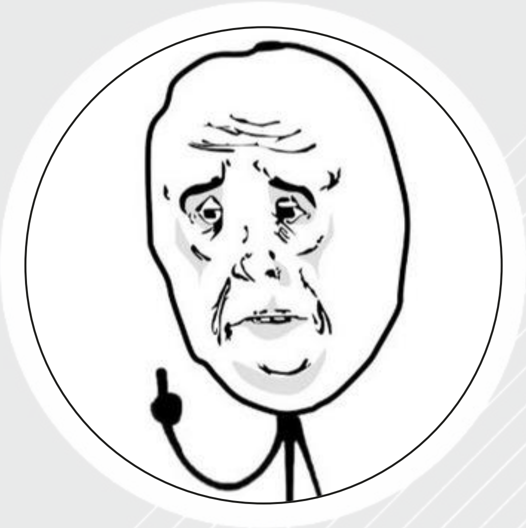
SPYWOLF

Security Audit Report



Completed on

July 25, 2023

@SPYWOLFNETWORK

@SPYWOLFNETWORK

SPYWOLF.CO

OVERVIEW

This audit has been prepared for **OkayGuy** to review the main aspects of the project to help investors make make an informative decision during their research process.

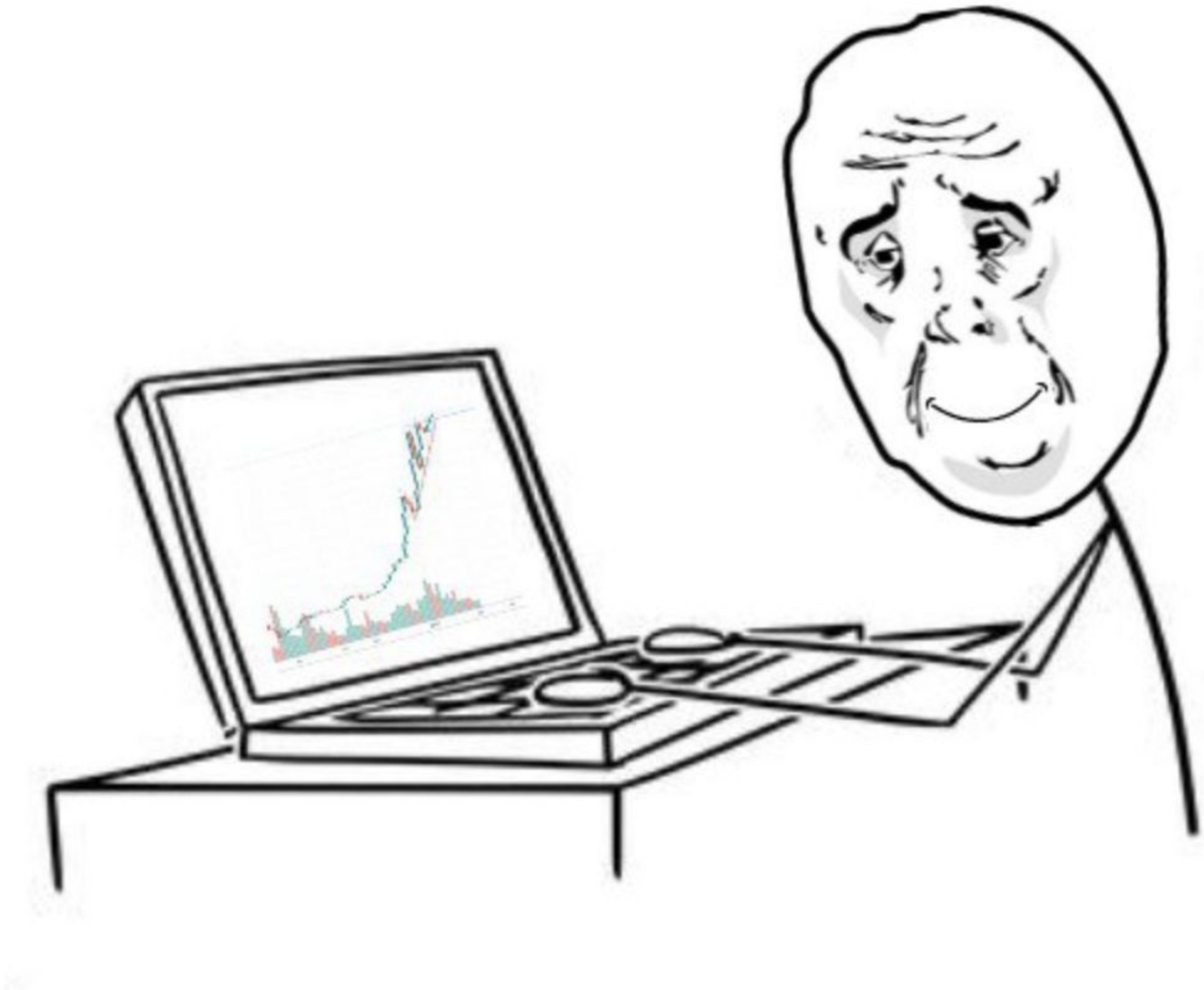
You will find a a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

> *The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal*
>
> - SPYWOLF Team -

TABLE OF CONTENTS

OkayGuy



PROJECT DESCRIPTION

According to their website:
After getting rugged, honeypotted, scammed, and generally losing money on bad crypto projects, Okay Guy was finally feeling more than okay because he aped into $OKAY.
He was so excited, he even started to think he was the Okay Guy. But then he remembered that he was still down 90% on his investment. So he went back to feeling just okay.

Release Date: Presale starts in July, 2023

Category: Meme token

CONTRACT INFO

Token Name
The OKAYGUY

Symbol
OKAYGUY

Contract Address
0x9786B287ba19636464410725dcD941f049Affb4a

Network
Binance Smart Chain

Language
Solidity

Deployment Date
JUl 24, 2023

Verified?
Yes

Total Supply
88,000,000,000

Status
Not launched

TAXES

Buy Tax
2%

Sell Tax
5%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	88000000000 OKAYGUY
Median Transfer Amount	88000000000 OKAYGUY
Average Transfer Amount	88000000000 OKAYGUY
First transfer date	2023-07-24
Last transfer date	2023-07-24
Days token transferred	1

SMART CONTRACT STATS

Calls Count	2
External calls	2
Internal calls	0
Transactions count	2
Uniq Callers	1
Days contract called	1
Last transaction time	2023-07-24 16:52:32 UTC
Created	2023-07-24 16:46:39 UTC
Create TX	0xa19e924919caf74d64012a3c9602200725028bb302c956fadd516d6b5856fc48
Creator	0xd4ac10284be0672689cf7c851a43997914661c96

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

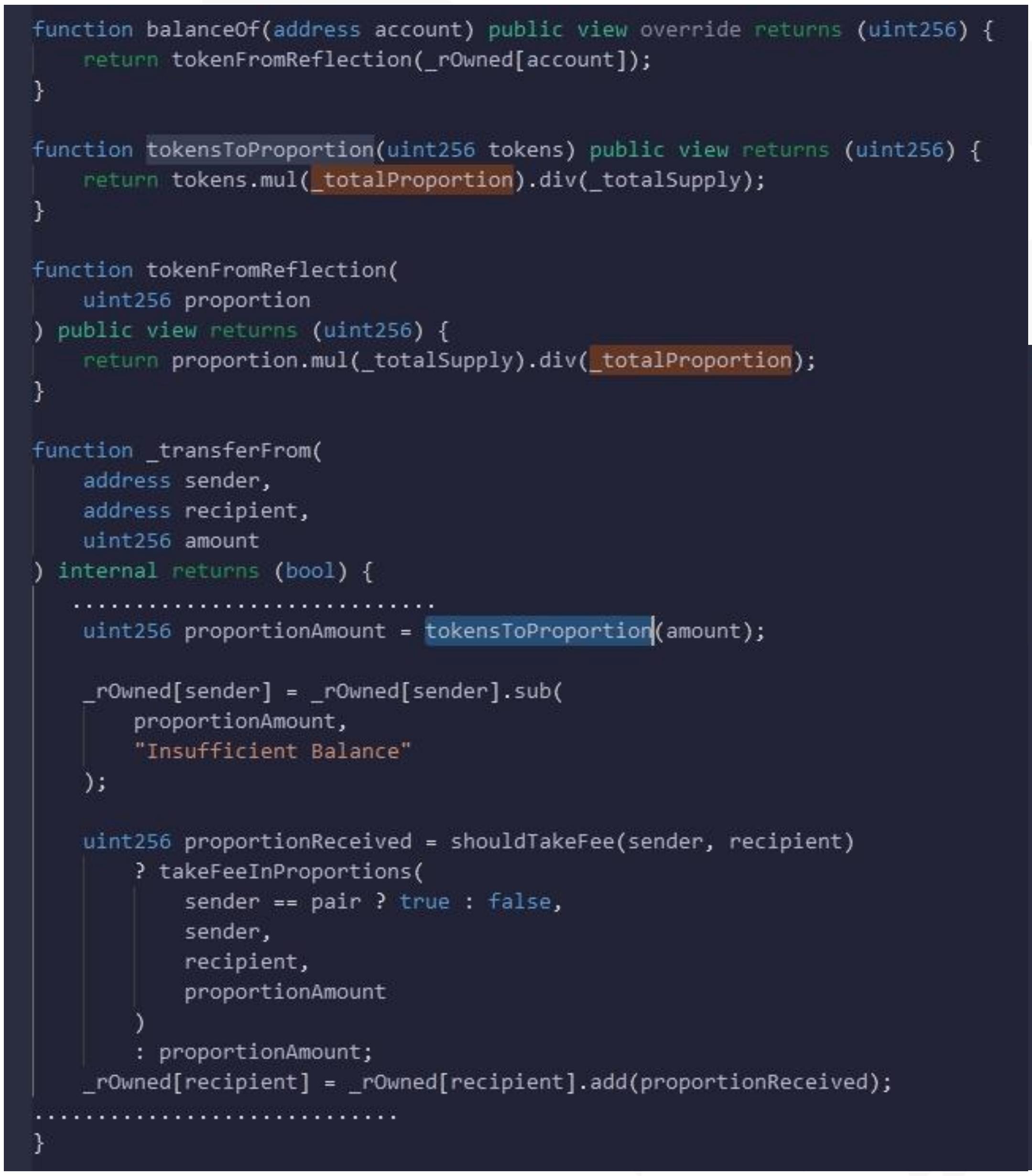
Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

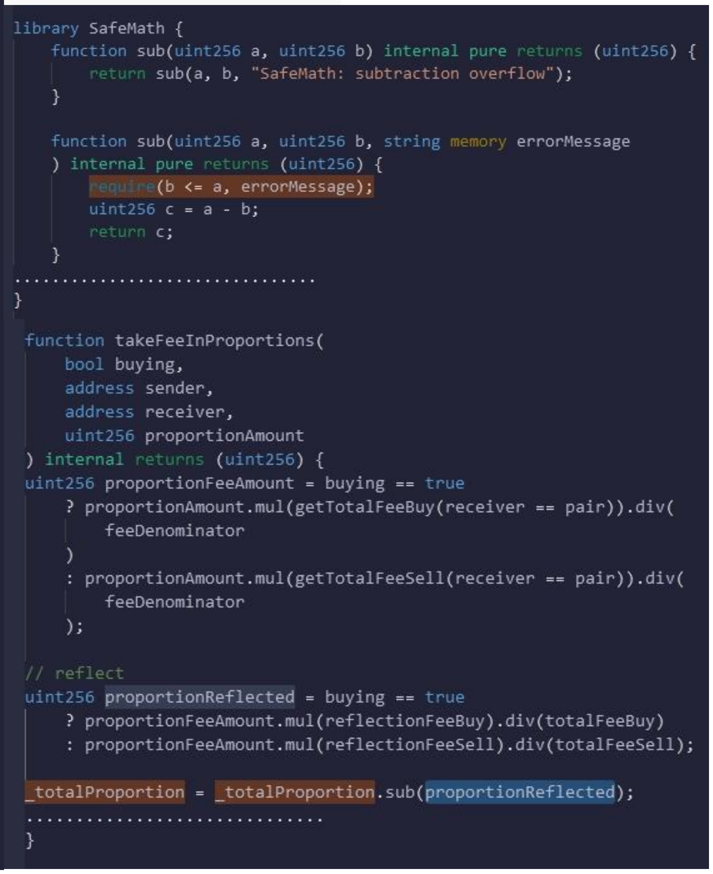
FOUND THREATS

⚠ High Risk

_totalProportion's value is always decreasing and if it reach 0, token will become untradeable and untransferable (divide/multiply by zero(0)). If _totalProportion's value become lower than the subtracted value, result will be negative number, causing the transaction to revert.



```
function balanceOf(address account) public view override returns (uint256) {
    return tokenFromReflection(_rOwned[account]);
}

function tokensToProportion(uint256 tokens) public view returns (uint256) {
    return tokens.mul(_totalProportion).div(_totalSupply);
}

function tokenFromReflection(
    uint256 proportion
) public view returns (uint256) {
    return proportion.mul(_totalSupply).div(_totalProportion);
}

function _transferFrom(
    address sender,
    address recipient,
    uint256 amount
) internal returns (bool) {
   ..............................
    uint256 proportionAmount = tokensToProportion(amount);

    _rOwned[sender] = _rOwned[sender].sub(
        proportionAmount,
        "Insufficient Balance"
    );

    uint256 proportionReceived = shouldTakeFee(sender, recipient)
        ? takeFeeInProportions(
            sender == pair ? true : false,
            sender,
            recipient,
            proportionAmount
        )
        : proportionAmount;
    _rOwned[recipient] = _rOwned[recipient].add(proportionReceived);
..............................
}
```



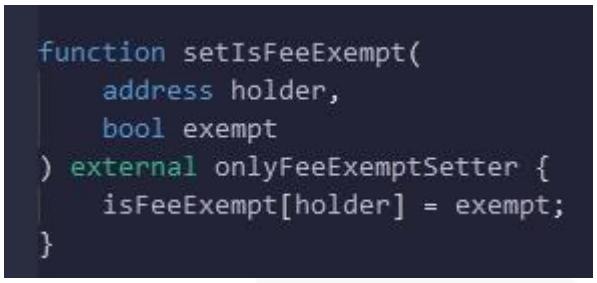
```
library SafeMath {
    function sub(uint256 a, uint256 b) internal pure returns (uint256) {
        return sub(a, b, "SafeMath: subtraction overflow");
    }

    function sub(uint256 a, uint256 b, string memory errorMessage
    ) internal pure returns (uint256) {
        require(b <= a, errorMessage);
        uint256 c = a - b;
        return c;
    }
................................
}

 function takeFeeInProportions(
     bool buying,
     address sender,
     address receiver,
     uint256 proportionAmount
 ) internal returns (uint256) {
 uint256 proportionFeeAmount = buying == true
     ? proportionAmount.mul(getTotalFeeBuy(receiver == pair)).div(
        feeDenominator
     )
     : proportionAmount.mul(getTotalFeeSell(receiver == pair)).div(
        feeDenominator
     );

 // reflect
 uint256 proportionReflected = buying == true
     ? proportionFeeAmount.mul(reflectionFeeBuy).div(totalFeeBuy)
     : proportionFeeAmount.mul(reflectionFeeSell).div(totalFeeSell);

 _totalProportion = _totalProportion.sub(proportionReflected);
 ..............................
 }
```

Recommendation

- when _totalProportion's value reaches 1% of total supply, reflection fees for buys and sells must be set to 0 and never turned on again.

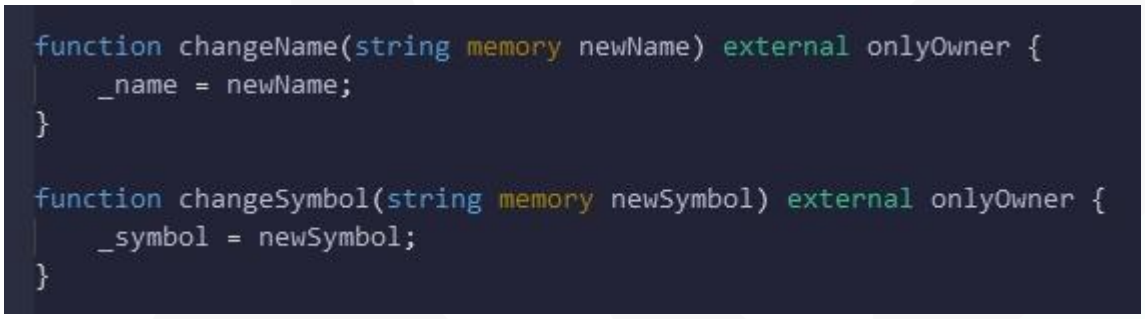
Informational

Owner can exclude address from fees.
When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.



```
function setIsFeeExempt(
    address holder,
    bool exempt
) external onlyFeeExemptSetter {
    isFeeExempt[holder] = exempt;
}
```

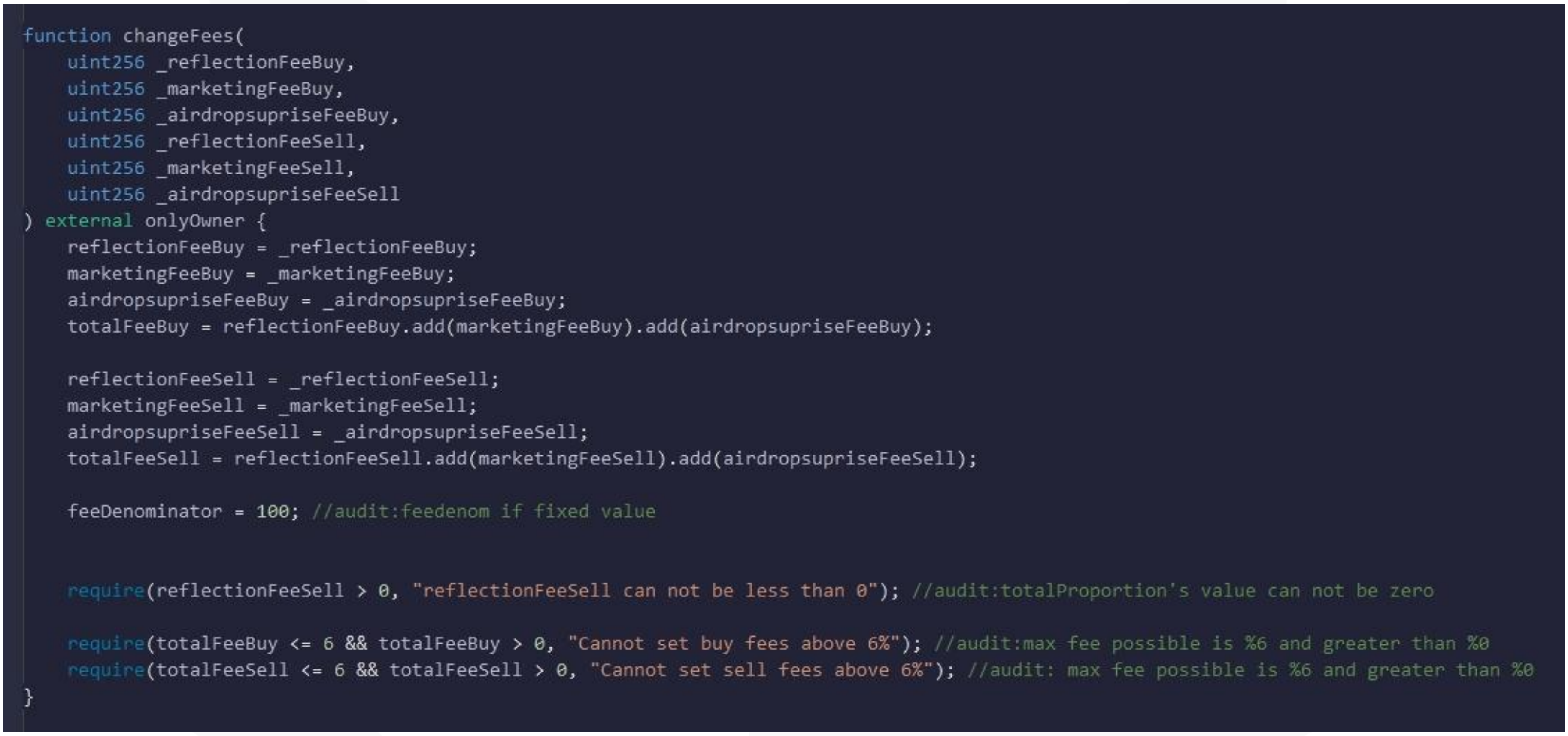
Owner can change token's name and symbol after deployment.
*Token's name and symbol should **not** be changed after deployment as it might cause confusion between investors and/or token explorers (like BSCScan).*



```
function changeName(string memory newName) external onlyOwner {
    _name = newName;
}

function changeSymbol(string memory newSymbol) external onlyOwner {
    _symbol = newSymbol;
}
```

Informational

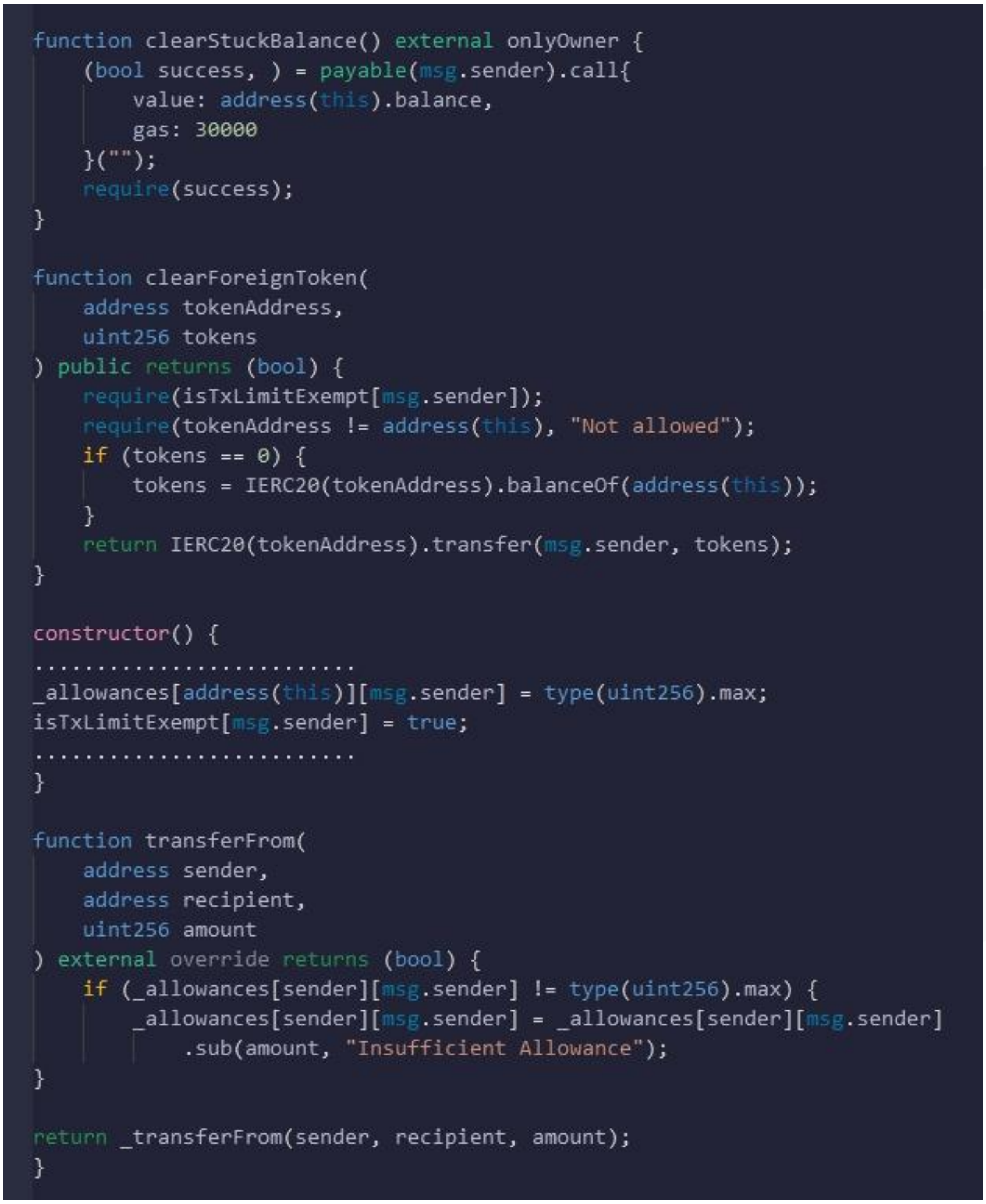
Owner can set buy/sell fees up to 6%.
Combined buy+sell = 12%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make. Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.



```
function changeFees(
    uint256 _reflectionFeeBuy,
    uint256 _marketingFeeBuy,
    uint256 _airdropsupriseFeeBuy,
    uint256 _reflectionFeeSell,
    uint256 _marketingFeeSell,
    uint256 _airdropsupriseFeeSell
) external onlyOwner {
    reflectionFeeBuy = _reflectionFeeBuy;
    marketingFeeBuy = _marketingFeeBuy;
    airdropsupriseFeeBuy = _airdropsupriseFeeBuy;
    totalFeeBuy = reflectionFeeBuy.add(marketingFeeBuy).add(airdropsupriseFeeBuy);

    reflectionFeeSell = _reflectionFeeSell;
    marketingFeeSell = _marketingFeeSell;
    airdropsupriseFeeSell = _airdropsupriseFeeSell;
    totalFeeSell = reflectionFeeSell.add(marketingFeeSell).add(airdropsupriseFeeSell);

    feeDenominator = 100; //audit:feedenom if fixed value


    require(reflectionFeeSell > 0, "reflectionFeeSell can not be less than 0"); //audit:totalProportion's value can not be zero

    require(totalFeeBuy <= 6 && totalFeeBuy > 0, "Cannot set buy fees above 6%"); //audit:max fee possible is %6 and greater than %0
    require(totalFeeSell <= 6 && totalFeeSell > 0, "Cannot set sell fees above 6%"); //audit: max fee possible is %6 and greater than %0
}
```

Informational

Owner can withdraw any tokens from the contract.
When this function is present, in cases tokens sent into the contract by mistake or purposefully, contract's owner can retrieve them.



```
function clearStuckBalance() external onlyOwner {
    (bool success, ) = payable(msg.sender).call{
        value: address(this).balance,
        gas: 30000
    }("");
    require(success);
}

function clearForeignToken(
    address tokenAddress,
    uint256 tokens
) public returns (bool) {
    require(isTxLimitExempt[msg.sender]);
    require(tokenAddress != address(this), "Not allowed");
    if (tokens == 0) {
        tokens = IERC20(tokenAddress).balanceOf(address(this));
    }
    return IERC20(tokenAddress).transfer(msg.sender, tokens);
}

constructor() {
..........................
_allowances[address(this)][msg.sender] = type(uint256).max;
isTxLimitExempt[msg.sender] = true;
..........................
}

function transferFrom(
    address sender,
    address recipient,
    uint256 amount
) external override returns (bool) {
    if (_allowances[sender][msg.sender] != type(uint256).max) {
        _allowances[sender][msg.sender] = _allowances[sender][msg.sender]
            .sub(amount, "Insufficient Allowance");
}

return _transferFrom(sender, recipient, amount);
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

OkayGuy

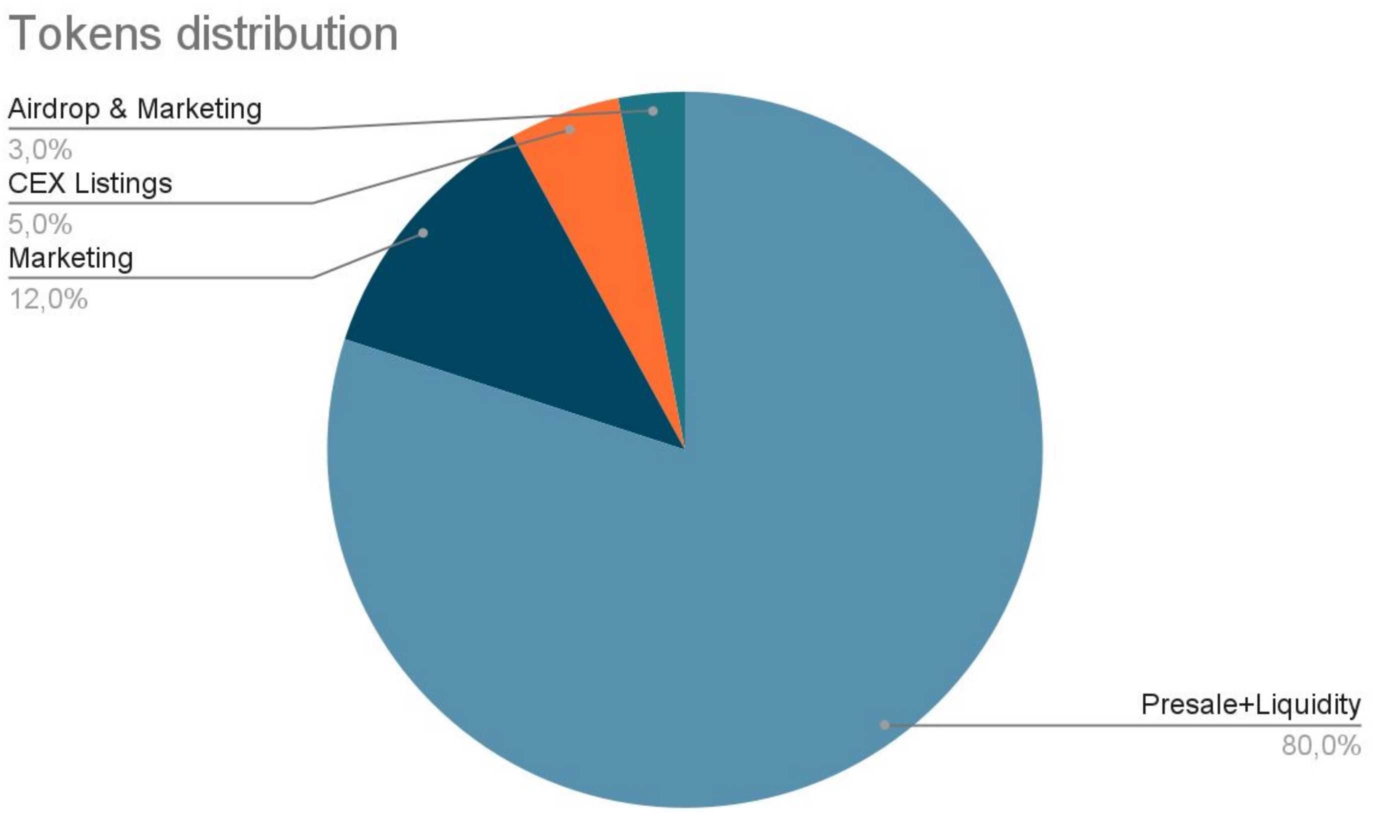
GOOD PRACTICES FOUND

- ✓ The owner cannot mint new tokens after deployment
- ✓ The owner cannot set a transaction limit
- ✓ The smart contract utilizes "SafeMath" to prevent overflows

TOKENOMICS

The following tokenomics are based on the project's whitepaper and/or website:

- 80% - Presale+Liquidity
- 12% - Team
- 5% - CEX Listings
- 3% - Airdrop & Marketing



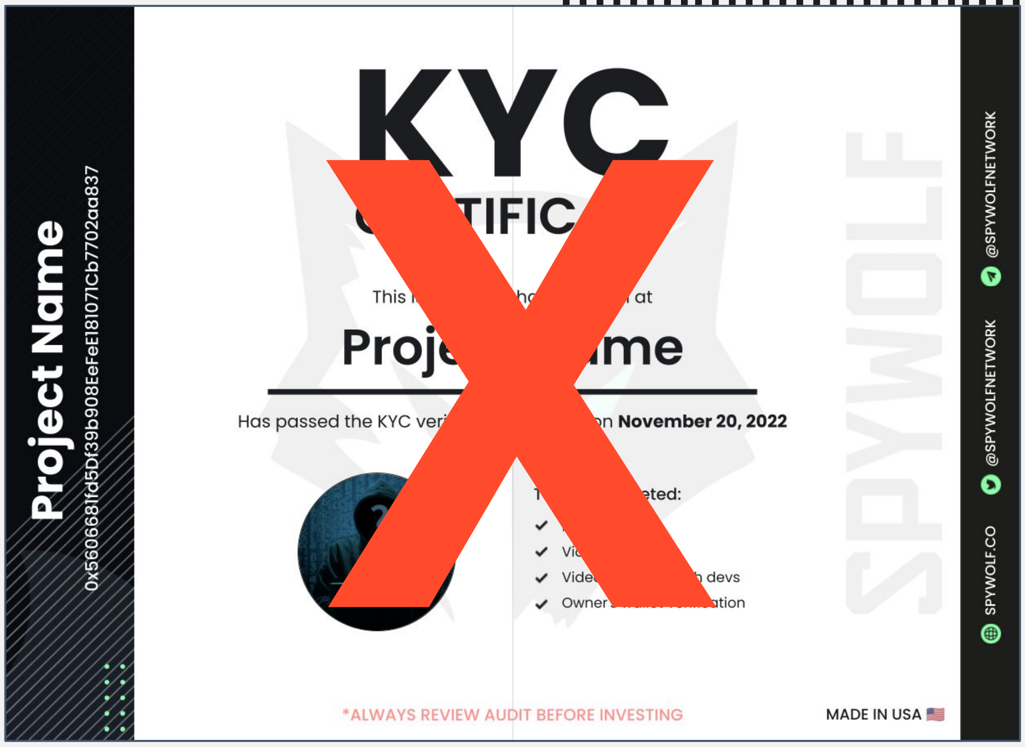
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



Project Name

0x5606681fd5Df39b908EeFeE181071Cb7702aa837

KYC

C TIFIC

This i ho at

Proje me

Has passed the KYC veri on **November 20, 2022**

T eted:

✓

✓ Vi

✓ Vide h devs

✓ Owner ation

*ALWAYS REVIEW AUDIT BEFORE INVESTING

MADE IN USA 🇺🇸

SPYWOLF
@SPYWOLFNETWORK
@SPYWOLFNETWORK
SPYWOLF.CO

WEBSITE

Website URL
https://okayguy.xyz/

Domain Registry
https://www.name.com/

Domain Expiration
2024-05-19

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

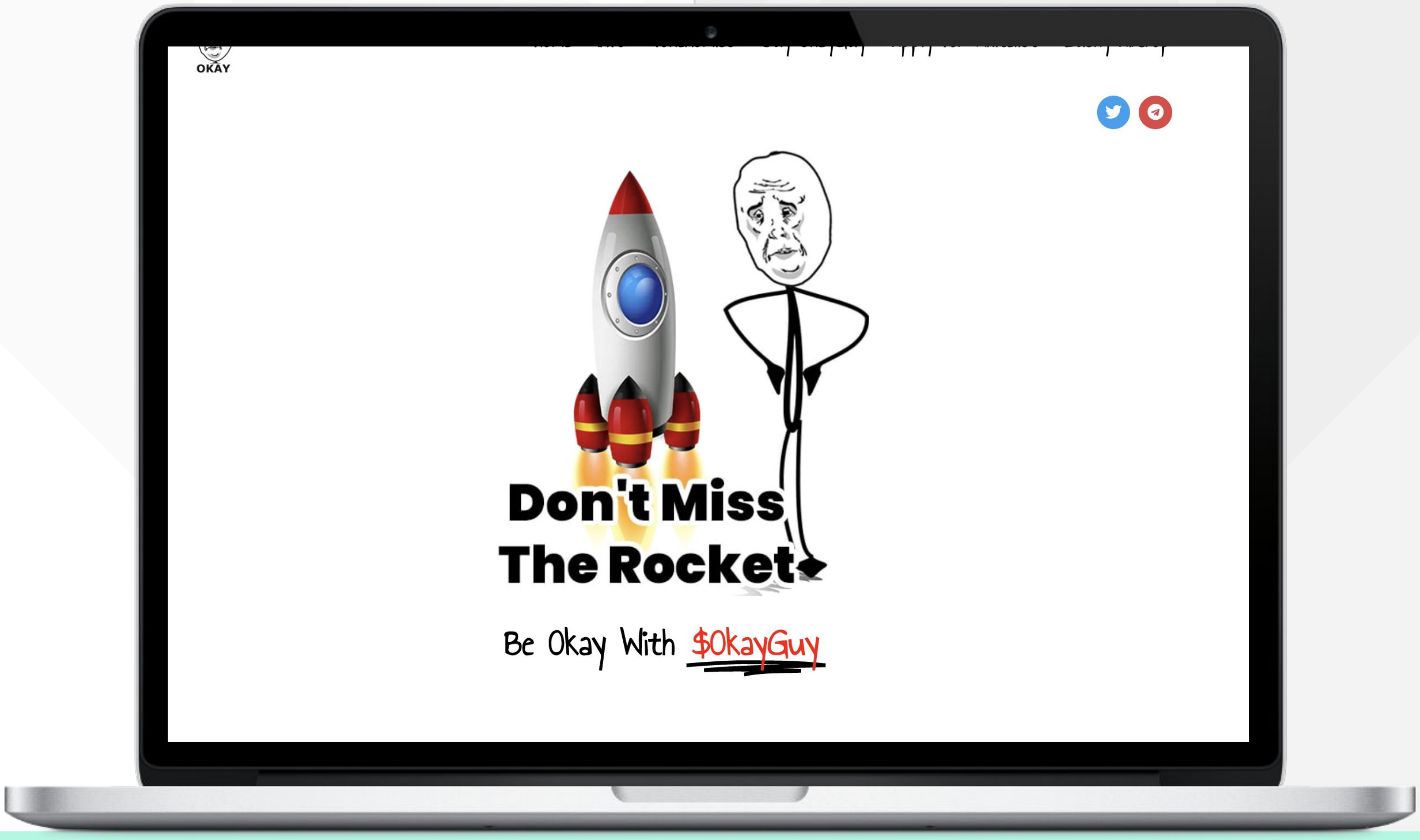
Design
Single page design with appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
No

Roadmap
No

Mobile-friendly?
Yes



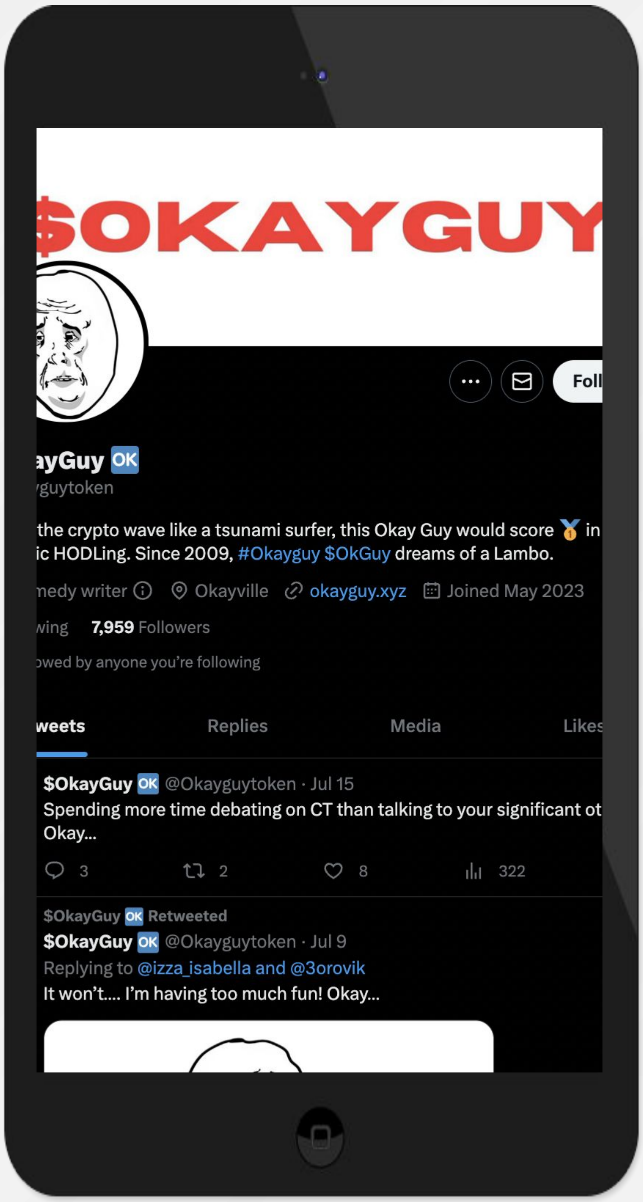
okayguy.xyz

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Social media pages are active with daily posts.



ayGuy OK
guytoken

the crypto wave like a tsunami surfer, this Okay Guy would score 🥇 in
ic HODLing. Since 2009, #Okayguy $OkGuy dreams of a Lambo.

nedy writer · Okayville · okayguy.xyz · Joined May 2023

wing 7,959 Followers

owed by anyone you're following

$OkayGuy OK @Okayguytoken · Jul 15
Spending more time debating on CT than talking to your significant ot
Okay...

3 · 2 · 8 · 322

$OkayGuy OK Retweeted
$OkayGuy OK @Okayguytoken · Jul 9
Replying to @izza_isabella and @3orovik
It won't.... I'm having too much fun! Okay...

Twitter

@Okayguytoken

- 7 977 followers
- Posts frequently
- Active

Discord

- Not available

Telegram

@okayguytoken

- 1 671 members
- Active members
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 500 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.